IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

JOHN DOE, on behalf of themselves and all others similarly situated Plaintiff v. PROMEDICA HEALTH SYSTEMS, INC. Defendant	CASE NO. 3:20-CV-01581 JUDGE JACK ZOUHARY

PLAINTIFF'S MOTION TO REMAND

Plaintiff John Doe moves this Court, pursuant to 28 U.S.C. § 1367, to remand this action to the Court of Common Pleas of Lucas County, Ohio. In support, Plaintiff states the following:

I. Nature of the Case

1. Plaintiff is a resident and citizen of Ohio and a patient of Defendant ProMedica, an Ohio corporation. All of Defendant's acts creating liability herein took place in Ohio.

2. On June 12, 2020, Plaintiff filed suit in the Lucas County Court of Common Pleas, alleging three Ohio common law torts: (1) disclosure of non-public medical information in violation of *Biddle v. Warren Gen. Hosp.*, 86 Ohio St. 3d 395 (1995); (2) breach of confidence; and (3) invasion of privacy. (Complaint attached hereto as **Exhibit A.**)

3. Plaintiff's Complaint alleges that Defendant purposefully disclosed Plaintiff's and other patients' personally identifiable, non-public medical information, and the contents of communications exchanged between patients and Defendant to Facebook, Google, Bing, and Quantcast through invisible web bugs for marketing purposes without obtaining patient consent or authorization. *See* Compl., at ¶¶ 5-10.

II. Defendant's Notice of Removal

4. On July 17, 2020, Defendant filed a Notice of Removal (Doc. 1), asserting that the allegations occurred in relation to its role as a "federal officer," thereby justifying federal officer removal under 28 U.S.C. § 1442(a)(1).

5. Defendant's Notice does not identify or provide any evidence of the following:

a. A delegation of authority to it from a federal officer;

b. A contract with a federal officer;

c. An employer/employee relationship with any federal officer;

d. A principal/agent relationship with any federal officer;

e. Direction or guidance from any federal officer directing Defendant to disclose patient personally identifiable data and communications to third parties for marketing purposes;

f. A duty for any federal officer to disclose patient personally identifiable data and communications to third parties for marketing purposes;

g. A duty for any federal officer (or hospital) to create a web property for patients;

h. A duty for any federal officer (or hospital) to create a patient portal;

i. A task or service which, in the absence of Defendant's help, a federal officer would have to perform itself; or

j. How the deployment of third-party marketing tools that causes disclosures to third parties is in any way related to the "Promoting Interoperability" Program, which Defendant erroneously refers to as the "Meaningful Use" Program.

6. Rather than provide the evidence necessary for removal under the federal officer statute, Defendant instead contends it "has acted within the penumbra of federal action and office." Doc. 1 at ¶ 11. But there is no "penumbra" test. Rather, a defendant must show (1) it is a party within the meaning of the statute, (2) it was "acting under" a federal officer; (3) the actions at issue were performed "under color of federal office," and (4) it has a colorable federal defense. *Mays v. City of Flint*, 871 F.3d 437, 442-43 (6th Cir. 2017). Defendant fails to meet elements 2 through 4.

III. Defendant Does Not Qualify for Federal Officer Removal Based on Its Disclosures of Patient Data to Facebook, Google, Microsoft, and Quantcast

A. ProMedica is Not "Acting Under" a Federal Officer

7. ProMedica's notice of removal relies on *Bennett v. MIS Corp*., 607 F.3d 1076 (6th Cir. 2010). Under *Bennett*, a court analyzes the following factors: "(1) whether the entity is 'helping the government to produce an item it needs;' (2) whether the federal government would handle the task on its own absent the private entity's involvement; (3) whether the government provided specifications for how the work should be done; and (4) whether the government closely monitored the private entity's conduct." Doc. 1 at ¶ 25 (citing *Bennett*, 607 F.3d at 1086-87). Here, none of these factors support removal.

8. By deploying third-party source codes on its web properties that cause the disclosure of patients' personally identifiable data and communications to Facebook and others for marketing purposes without authorization, Defendant is not "helping the government to produce an item it needs." *Id.* The federal government does not need to advertise private hospitals to patients. More broadly, the government does not need Defendant's web property or patient portal. In fact, the Promoting Interoperability Program does not even require hospitals to maintain a website or patient portal. CMS, *EHR Incentive Program Stage 3 Rule*, 80 FR 62842 (Oct. 16, 2015).

9. The federal government has not provided any specifications on how a hospital should organize or build a web property under the Promoting Interoperability Program. Indeed, Defendant's unilateral removal of much of the offending source code soon after Plaintiff filed suit belies the notion that its use occurred while "acting under" any federal agency or officer. *See* Declaration of Richard M. Smith (attached hereto as **Exhibit B**).

10. No federal agency or officer monitors hospital web properties and no federal agency or officer monitors hospital patient portals. Instead, a hospital that voluntarily participates in the Promoting Interoperability Program must merely "attest" that it is complying with privacy standards for such portals. 42 C.F.R. § 495.40(b)(2)(i).

B. Defendant's Disclosures to Facebook and Others for Marketing Purposes are Not *For or Relating to an Act Under Color of Federal Office*

11. To satisfy this element, "the removing party must show that it is being sued because of acts it performed at the direction of the federal officer." *Bennett*, 607 F.3d at 1088.

12. Here, Plaintiff's claims relate to Defendant's deployment of third-party source code from Facebook and others through which Defendant discloses personally identifiable data and communications about patients for marketing purposes, including confidential medical data.

13. Defendant has not presented evidence that any federal agency or officer directed it to place third-party source code on its web property or patient portal. Indeed, the federal officers and agencies cited by Defendant have the opposite duty: to protect patient privacy. For example:

a. The primary purpose of Executive Order 13335, cited by Defendant as creating the National Health Information Technology Coordinator (ONC), is to "ensure[] that patients' individual identifiable health information is secure and protected." E.O. 13335 § 2(f) at 703.

b. The HITECH Act, cited by Defendant, codified the existence of the ONC, explained that ONC must perform its duties "in a manner … that (1) ensure[s] that each patient's health information is secure and protected, in accordance with applicable law." 42 U.S.C. § 300jj-11. The Act further directed HHS to "support the nationwide electronic exchange and use of health information in a secure, private, and accurate manner" and to "promot[e] technologies and best practices that enhance the protection of health information by all holders of individually identifiable information." 42 U.S.C. § 300jj-31(a)(1). The Act clarified that the incentive programs created did not supplant HIPAA, 42 U.S.C. § 300jj-19, and established "stronger restrictions on disclosing health information for marketing and fundraising purposes." ONC Health IT Strategic Plan 2010-15 at 30. Specifically, a covered entity may not "directly or indirectly" receive "remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual … a valid authorization" under HIPAA; 42 U.S.C. § 17935.

c. The ONC Strategic Plan 2015-2020, cited by Defendant, explains that to "help cultivate patients' trust," providers "should … carefully handle patients' health information secure their privacy." ONC 2015-2020 Guide at 3-9.

C. Defendant Does Not Present a "Colorable" Federal Defense

14. A claim or defense is "without color" when it "lacks any legal or factual basis … considered in light of the reasonable beliefs of the individual making the claim" or defense. *First Bank of Marietta v. Hartford Underwriters Ins. Co.*, 115 F.Supp.2d 898, 905 (S.D. Ohio 2000).

15. In this case, Defendant's proffered defenses are not colorable, and, in the case of the applicability of HIPAA to the underlying causes of action, not federal in nature.

16. Defendant argues that "traffic on ProMedica's website is not covered by" HIPAA and "that the information that is purportedly disclosed (*i.e.* IP address and other web metadata) are outside of the purview of protected health information" as defined by HIPAA. Doc. 1 at ¶ 38. This misunderstands Plaintiff's Complaint. Plaintiff brings suit on behalf of all Ohio residents who "are, or were, patients of ProMedica or any of its affiliates and who used ProMedica's web properties, including but not limited to, www.promedica.org and the Patient Portal at MyChart." Compl. ¶ 249. Patient communications included logins to the patient portal (which, by their nature, identify patient status), communications within the Patient Portal, and communications about treatments, providers, conditions, and risk assessments. Compl. ¶¶ 130-195, 267.

17. Under HIPAA, a healthcare provider may not disclose individually identifiable health information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express authorization. 42 U.S.C. § 1320d-6, 45 C.F.R. §§ 164.501; 164.508(a)(3); 164.514(b)(2)(i). Furthermore, the HIPAA Privacy Rule provides that "individually identifiable health information" means "any information, including demographic information, collected from an individual that—(A) is created or received by a health care provider …; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment

for the provision of health care to an individual, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. § 1320(d)(6); 45 C.F.R. § 160.103.

18. HHS has provided categories of data considered identifiable as a matter of law, including, but not limited to, the following categories: *names*, phone numbers, email addresses, medical record numbers, *account numbers*, *device identifiers*, and serial numbers, Web Universal Resource Locators (URLs), and *IP addresses*. 45 C.F.R. § 164.514(b)(2)(i).

19. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*.[1]

20. This HIPAA guidance from HHS is consistent with the plain language of the statute, rules, and HHS's comments in various rulemakings. For example:

a. In its initial rulemaking, HHS clarified, "[T]he sale of a patient list to a marketing firm … would not be permitted under this rule without authorization from the individual." 65 F.R. 82717 (Dec. 28, 2000).

b. Two years later, HHS specified that "a covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications and will no longer be able to do

[1] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (emphasis added).

so simply by meeting the disclosure and opt-out provisions previously set forth in § 164.514(e).” 67 FR 53186 (Aug. 14, 2002).

c. Then, in its 2013 Omnibus Rulemaking, HHS explained that it would be a violation “if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers.” In such a situation, “the protected health information is obviously identifiable … .” 78 FR 5642 (Jan. 25, 2013).

21. Finally, Defendant claims it has a colorable argument that HIPAA preempts Ohio law. Not so, as HIPAA and the federal officers to which Defendant points for federal officer removal specifically state that HIPAA does not preempt state privacy laws that are at least as protective as HIPAA. HIPAA establishes floor preemption, which does not apply where “[t]he provision of state law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted” under the HIPAA Privacy Rule. 45 C.F.R. § 160.203(b). As the ONC has explained, providers “need to be aware of … additional applicable federal, state, and local laws governing the privacy and security of health information” because “[s]tate laws that are more privacy-protective than HIPAA continue to apply.” ONC, *Guide to Privacy and Security of Electronic Health Information* at 21.[2]

[2] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

CONCLUSION

For the foregoing reasons, Plaintiff requests that the Court remand this case to the Lucas County Court of Common Pleas.

Respectfully submitted,

s/ Kevin C. Hulick
STUART E. SCOTT (0064834)
KEVIN C. HULICK (0093921)
SPANGENBERG SHIBLEY & LIBER LLP
1001 Lakeside Avenue East, Suite 1700
Cleveland, OH 44114
(216) 696-3232
(216) 696-3924 (FAX)
sscott@spanglaw.com
khulick@spanglaw.com

MITCHELL BREIT (*pro hac vice*)
JASON 'JAY' BARNES (*pro hac vice*)
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016-7416
(212) 784-6400
(212) 213-5949 (FAX)
mbreit@simmonsfirm.com
jaybarnes@simmonsfirm.com

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 17th day of August 2020, I electronically filed the foregoing with the Clerk of Court by using the CM/ECF System. Copies will be served upon counsel of record by, and may be obtained through, the Court CM/ECF Systems.

s/ Kevin C. Hulick
STUART E. SCOTT (0064834)
KEVIN C. HULICK (0093921)
SPANGENBERG SHIBLEY & LIBER LLP
1001 Lakeside Avenue East, Suite 1700
Cleveland, OH 44114
(216) 696-3232
(216) 696-3924 (FAX)
sscott@spanglaw.com
khulick@spanglaw.com

Counsel for Plaintiff and the Proposed Class